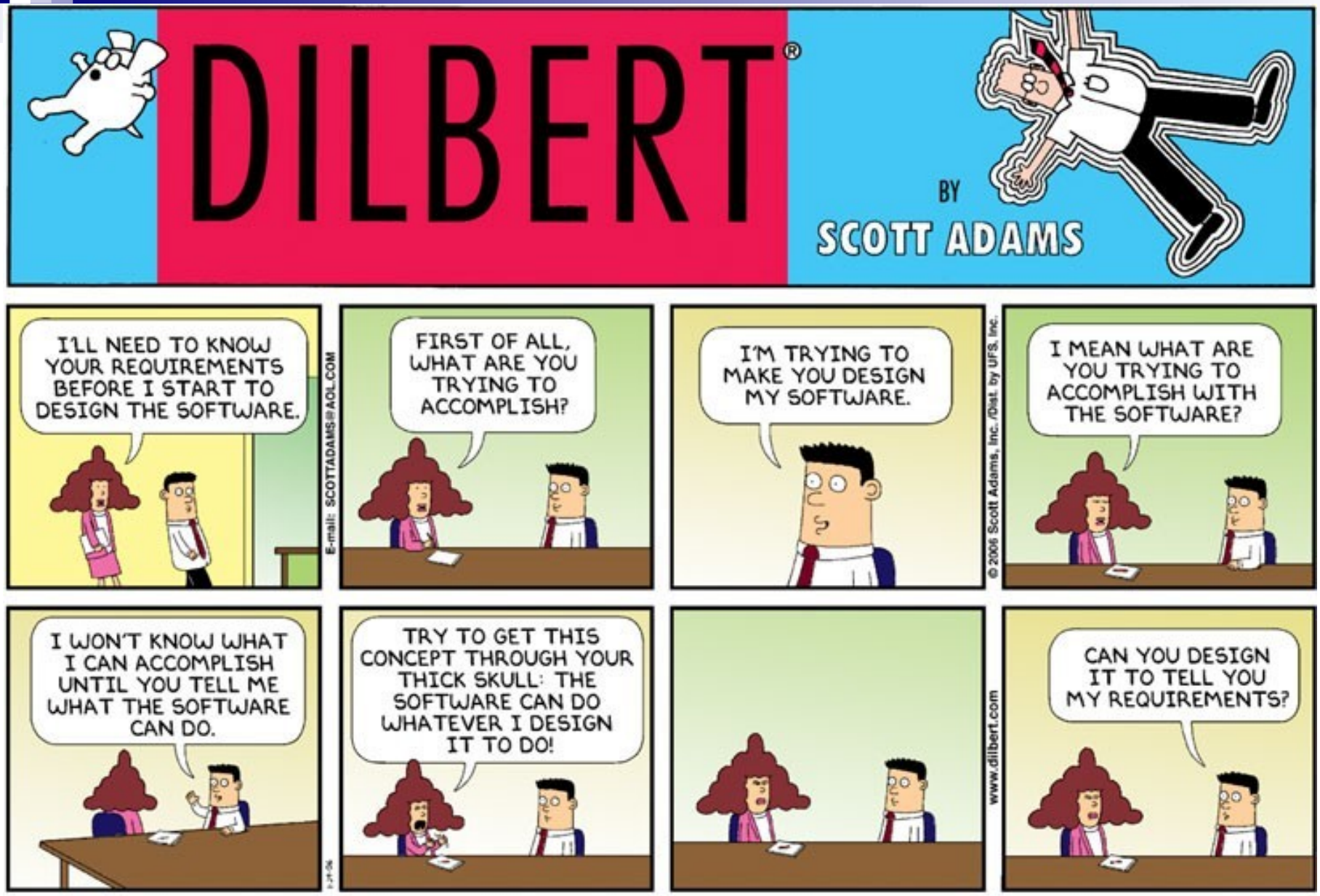
STATES AND MODES WG-6

Unmanned Vehicle System Safety Workshop

STATES AND MODES TEAM

Moderator	Schmedake, Bob	(314) 232-0552	robert.a.schmedake@boeing.com	Army, CTR Boeing
Scribes	Hosner, Steven	256-461-7074 Ext. 305	steven.hosner@L-3Com.com	
	Fay, Bart	256-230-1610	fay@westar.com	
Tech Participants	Brown, Mike	(831) 449-0498	michaelbrown7935@sbcglobal.net	Navy, CTR EG&G
	Butler, Jim	(256) 842-2709	james.a.butler@us.army.mil	AMREDEC SED, GOV'T
	Emery, Melissa	(256) 842-8635	melissa.emery@us.army.mil	USMC, CTR AOT
	Pfledderer, Lynece		lynece.pfledderer@lmco.com	Army, FCS
	Wade, Robert	(256) 842-6174	robert.l.wade@us.army.mil	AMREDEC SED, GOV'T
	Zarzycki, Henry	(973) 724-4550	henry.zarzycki@us.army.mil	Army, Picattiny


DILBERT®
BY
SCOTT ADAMS
I'LL NEED TO KNOW YOUR REQUIREMENTS BEFORE I START TO DESIGN THE SOFTWARE.
E-mail: SCOTTADAMS@AOL.COM
FIRST OF ALL, WHAT ARE YOU TRYING TO ACCOMPLISH?
I'M TRYING TO MAKE YOU DESIGN MY SOFTWARE.
© 2006 Scott Adams, Inc./Dist. by UFS, Inc.
I MEAN WHAT ARE YOU TRYING TO ACCOMPLISH WITH THE SOFTWARE?
I WON'T KNOW WHAT I CAN ACCOMPLISH UNTIL YOU TELL ME WHAT THE SOFTWARE CAN DO.
TRY TO GET THIS CONCEPT THROUGH YOUR THICK SKULL: THE SOFTWARE CAN DO WHATEVER I DESIGN IT TO DO!
www.dilbert.com
CAN YOU DESIGN IT TO TELL YOU MY REQUIREMENTS?

© Scott Adams, Inc./Dist. by UFS, Inc.

BACKGROUND

- Workgroup Assignment
  - Review precepts and TLMs from the perspective of States and Modes for unmanned vehicles.
- Unique Assumptions
  - Vocabulary of states and modes not standardized
  - Often used interchangeably

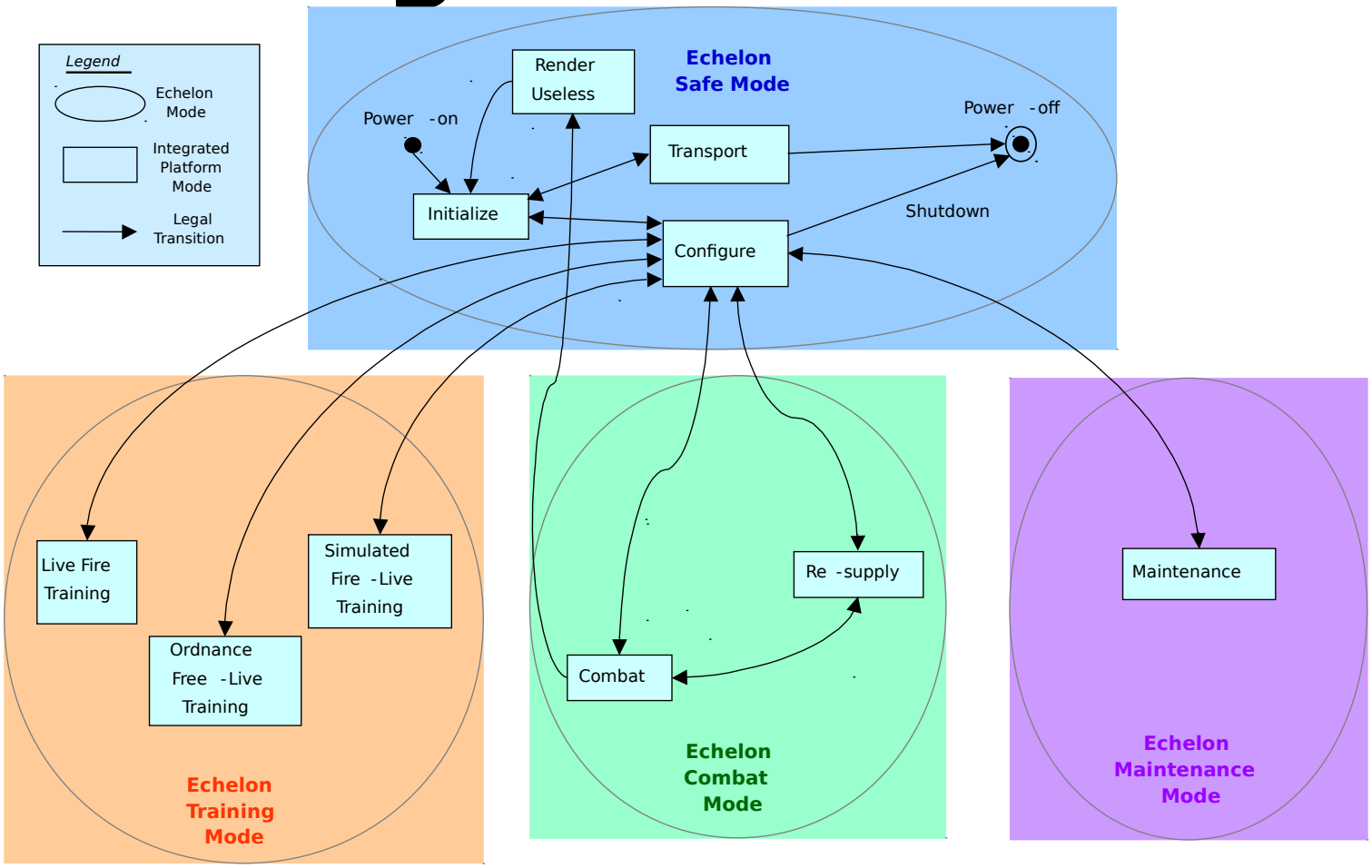
Terms of Reference

- Mode: Modes identify operational segments within the system lifecycle generally defined in the Concept of Operations. Modes consist of one or more sub-modes. A system may be in only one mode but may be in more than one sub-mode at any given time.

Terms of Reference

- Modes include: logistic mode, pre-deployment mode, tactical mode, training mode, return and recovery, maintenance, etc.
- Sub-modes of the tactical mode may include ISR, BDA, Weapon Guidance, Weapon delivery, etc.

Mode Transition Diagram



Terms of Reference

- State: States identify conditions in which a system or subsystem can be said to exist exclusively. A system or subsystem may be in only one state at a time. States are unique and may be binary (i.e., they are either true or not true). Allowable system and subsystem states need to be defined for each mode/ sub-mode during development.

Terms of Reference

- Safe State: A state in which the system poses an acceptable level of risk for the operational mode.
  - Weapons armed is not a safe state during logistics and pre-deployment modes
  - Weapons armed is a “safe state” when engaging a target (except to the enemy)

BACKGROUND

- Critical Issues Identified and Addressed
  - Mode Transition Control
  - Mode Confusion
  - State Transition
  - Unsafe Combinations of modes and states
  - Contingencies
  - Control Transfer
  - Warm Start
  - System of systems-level mode/ state

Issue Description
Issue #1: Mode Transitions

- Rationale for Selecting Issue
  - Highly critical hazards may be associated with mode transitions
  - Current DSPs and OSPs marginally address this issue
- Issue Description
  - Transitions between modes or sub-modes change the operational characteristics and associated states of the UV
  - Mode transitions may cause UV to enter unsafe states, perform unintended operations or not properly clear state information
  - Examples:
    - Out of sequence
    - Inadvertent transitions
    - Residual data or control command

Issue Resolution: Mode Transitions

- Applicable TLM/Precepts
  - OSP-1: Mode and sub-mode transitions change operations and/or states
  - OSP-2: Operator may control mode and state transitions
  - OSP-4: The system shall be in a verifiable safe state before transitioning between high-level operational modes: sub-mode transitions may occur without verification of safe state if the resulting sub-mode is “safer” in the operational context.
    - e.g., UAV may fly in circular pattern (sub-mode of tactical mode) if communications lost without verifying safe state of UAV

Issue Description: Mode Transitions

- OSP-5: Defines a sub-mode and state
- DSP-4: Includes knowledge of mode, sub-mode and state: essential to mode and sub-mode transition control
- DSP-5: Control of transition between sub-modes and states
- DSP-7 through DSP-12: Control of transition between sub-modes and states
- DSP-16: Control of transition between sub-modes and states

- Design Requirement
  - There shall be positive control of transitions between operational modes and between sub-modes when the resultant sub-mode is a higher level of readiness (e.g., less safe)

Issue Description
Issue #2: Mode Confusion

- Definition: Mode confusion is incorrect/ erroneous awareness of the operational mode of system components at the subsystem, system, or system of systems level.
- Issue: Mode confusion may lead to any of the top-level mishaps.
- Rationale: Mode confusion can lead to any of the top-level mishaps. Mode confusion may occur within the UV, with the controller (not being aware of the UV operational mode), or in a system of systems, particularly if it is capable of tactical and training operations simultaneously (e.g., mode confusion leads to attacking training targets). Mode confusion may result from mixed operating modes, improper or incomplete transfers between modes, data latency, residual data, failures, transfer of control failure, etc.

Issue Resolution

- Safety Precepts
  - DSP-4: Includes knowledge of mode, sub-mode and state: essential to preventing mode confusion
  - DSP-8: Directly addresses issue
- Expansion on DSP-8
  - Safe mode and state combinations are mission and scenario dependent and should be identified through analyses.

Issue Description
Issue #3: State Transition Control

- Rationale: Transitions between subsystem states change the state of the system.

- Issue: Inadvertent or out-of-sequence transitions between states may result in any of the top-level mishaps. Transitions occurring without proper setup may result in any of the top-level mishaps

Issue Resolution

- Safety Precepts
  - OSP-2: Operator may control mode and state transitions
  - OSP-3: Defines requirement for state change
  - OSP (new): The system shall be in a verifiable safe state before transitioning between high-level operational modes: sub-mode transitions may occur without verification of safe state if the resulting sub-mode is “safer” in the operational context.
    - e.g., UAV may fly in circular pattern (sub-mode of tactical mode) if communications lost without verifying safe state of UAV
    - Higher level of abstraction of OSP-4

Issue Resolution

- Safety Precepts
  - OSP-5: Defines a sub-mode and state
  - DSP-4: Includes knowledge of mode, sub-mode and state: essential to state transition control
  - DSP-5: Control of transition between states
  - DSP-7 through DSP-10: Control of transition between states
  - DSP-12: Control of transition between states
  - DSP-16: Control of transition between states
    Provide Recommended wording

Issue Resolution

- Design Requirement
  - There shall be positive control of transitions between states if the resultant state is a higher level of readiness (e.g., armed weapon)
  - Transitions out of safe states shall comply with applicable design criteria and requirements (e.g., military standards for weapons)

Issue Description

Issue #4 Unsafe Combinations of modes and states

- Rationale for Selecting Issue
  - See Mode Confusion
  - Applies to all top-level hazards
- Issue Description
  - Mode confusion may lead to any of the top-level mishaps.
- Addressed by DSP-8

Issue Description
Issue #5: Contingencies

- Definition: Contingencies include end-game planning, loss of communications and control, and graceful degradation

Issue 5a: End Game

- Definition: Return and recovery mode of operation or operational termination
  - System of systems, system, mission, and scenario dependent
  - Includes: mission abort, system and/or system of systems failure, self-destruct, render useless, safe return, sterilization, remote control failure, etc.
- Rationale: Contingency planning and recovery planning need to be included in design considerations and mission planning
- Issue: Precepts do not address End Game operations or scenarios

Issue Resolution

- Recommended design and operational safety precepts:
  - DSP (new): Unmanned vehicle design shall include capabilities for end game scenarios as appropriate for the unmanned vehicle system
  - OSP (new): Mission planning shall address contingency scenarios as appropriate for the unmanned vehicle system

Issue Description

Issue #5b: Loss of Communication and Control

- Issue[1]: Loss of situational awareness by operator, including system modes and sub-modes and system and subsystem states. Inability by operator to intervene and control UV to preclude hazardous events.

- Rationale: System needs to accommodate loss of communications and control without creating a hazardous condition

1. Addressed only from perspective of modes and

Issue Resolution

- Resolution: System should enter safe state upon loss of communication and control consistent with the mission plan.
- Precepts:
  - OSP-1: maintaining situational awareness
  - OSP-2: operation by only authorized operator
  - OSP-3: verification of safe state
  - DSP-2: respond to operator commands
  - DSP-3: control by only authorized operator
  - DSP-4: situational awareness feedback

Issue Resolution

- Precepts Continued
  - DSP-7: uncommanded fire/release of weapons
  - DSP-8: prevent hazardous system mode combinations
  - DSP-9: abort weapon firing sequence
  - DSP-10: safely change modes and states
  - DSP-12: positive means to identify system state
  - DSP-13: no single point or common mode failures

Issue Description
Issue #5c: Graceful Degradation

- Definition: Maintaining a safe system state through reconfiguration due to failures in either the system of systems, the control system, the UV system, or the subsystems of the UV.
- Rationale: Operational necessities may require that the UV complete its mission or aspects of this mission despite the presence of failures e.g., UAV must continue surveillance mission despite loss of a sensor

Issue Resolution

- Issues: Precepts do not address Graceful Degradation of UV Systems or System of Systems
  - Sub-issues
    - Ability to detect failures accurately enough to reconfigure system
    - Notifying operators to allow appropriate decision making
    - Autonomous functions (sub-modes)

Issue Resolution

- Recommended design and operational safety precepts:
  - DSP (new): The reconfiguration capability, when implemented, shall ensure that the UV remains in a safe state for the operational mode.
    - Guidance: Unmanned vehicle design shall include designed-in reconfiguration as required by the unmanned vehicle system requirements documents.
  - OSP (new): Mission planning shall address contingency scenarios as appropriate for the unmanned vehicle system and mission
    - Same as for End Game

Issue Description
Issue #6: Control Transfer

- Definition: Transfer of an UV from one authorized operator to another (e.g., launch platform operator to field commander)
- Rationale: UV system must remain in its operating mode and in a safe state through control transfers
- Issues: Loss of situational awareness by the accepting operator, loss of situational awareness at the system level, UV mode confusion, inadvertent mode transitions, inadvertent state changes,
- Affects all top level mishaps

Issue Resolution

- Applicable precepts
  - OSP-1: maintain situational awareness – need to extend to cover both operator and system
  - OSP-2: only authorized and intended operators may assume control of UV
  - OSP-3: verifying safe state
  - OSP-6: qualified personnel
  - DSP-2: remain operational and respond to authorized operator commands
  - DSP-3: control only by intended operator

Issue Resolution

- Applicable precepts
  - DSP-4: control feedback to maintain situational awareness
  - DSP-8: positive measures to preclude hazardous mode and state combinations
  - DSP-9: weapon fire sequence abort: return to safe state
  - DSP-10: safe changing of modes and states
  - DSP-12: positive determination of system state

Issue Description

Issue #7: Warm Start

- Definition: rebooting a computer or other computational device as a result of detected failures during an operational mode (if not prohibited by system requirements specification)
- Rationale: errors and failures may result in a timeout condition (watchdog timer) or other condition requiring the computer to restart during a mission.
- Issues: The UV must remain in a safe state throughout the warm start. This requires determining:
  - When warm starts are appropriate,
  - What data needs to be retained and the senescence of the data in case of a restart,
  - The operational mode and sub-mode(s) before and after the warm start, and
  - The safe state for a warm start for the mode and sub-mode(s).

Issue Resolution

- Precepts
  - OSP-1: situational awareness
  - OSP-2: regaining control by intended operator
  - OSP-3: verification of safe state
  - DSP-3: regaining control by intended operator
  - DSP-4: control and situational awareness feedback
  - DSP-8: hazardous mode combinations
  - DSP-9: abort fire sequence
  - DSP-10: safely change modes and states
  - DSP-12: positive means to determine state

Issue Description

Issue #8: System of Systems

- Definition: Complex, loosely coupled heterogeneous systems intended to enhance situational awareness and mission effectiveness through synergism. Individual systems interface through a variety of communication media. The system of systems may or may not have a centralized command and control center.
- Rationale: Modern battlefield operations require interfacing heterogeneous systems to control the battlespace and effectively prosecute the battle. Unmanned vehicles will be an integral part of the system of systems for ISR, BDA, weapon guidance, weapon

Issue Description

- Potential to affect all TLMs
- Sub-issues:
  - Rules of Engagement control
  - Communications & control loss
  - Quality of service/ tradeoffs
    - Data integrity/ information assurance
    - Data latency/ senescence
    - Data security
  - Priority structure
  - Error in UV selection/ data transfer
  - Control Integrity
    - Control security
    - Control transfer
  - IFF/ Friendly fire mitigation

SoS: Rules of Engagement control

- Issues: Rules of engagement will determine allowable UV modes and sub-modes.
- Rationale: Changes in the rules of engagement will result in changes to modes and sub-modes. Maintaining control of mode and sub-mode transitions, especially from close control to semi-autonomous control to autonomous control.
- Resolution: See mode transitions and mode confusion for recommendations

SoS: Loss of Communications & Control

- Issue: Loss of situational awareness by operator, including system modes and sub-modes and system and subsystem states. Inability by operator to intervene and control UV to preclude hazardous events.
- Rationale: Loss of communications or control will result in loss of situational awareness by the operator, including mode and sub-mode identification and system and sub-system state.
- Resolution: See Loss of Communications & Control under Contingencies

SoS: Quality of service/ tradeoffs

- Definition: Quality of service includes data integrity, data security, and the timeliness of the data (data latency/ senescence) including control functions

- Issue[1]: communications must be sufficiently robust, timely, and secure to preclude unsafe mode or state transitions.

1. Addresses issue only from modes and states perspective

SoS: Data integrity/ information assurance

- Issue: Corrupt data can lead to any of the top level mishaps
- Rationale: errors in communications may result in unsafe UV operation
- Issue unresolved: deferred to C2 group

SoS: Data latency/ senescence

- Issue: data latency affects the quality and viability of data
- Rationale: delays in communications may result in unsafe UV operation, erroneous situational awareness
- Issue unresolved: deferred to C2 group
- Resolution:
  - Ability to intervene and regain control: See also loss of communications/ control

SoS: Data Security

- Issue: security of communications with UAV
- Rationale: insecure data may result in loss of control by the intended operator and unsafe mode or state transitions
- Issue unresolved: deferred to C2 group

SoS: Priority Structure

- Issue[1]: safety-critical messages may require higher priority to preclude transitions to hazardous modes, sub-modes, states or combinations thereof and transition the system to a safe state.
- Rationale: safety-critical messages not acted upon in a timely manner may result in a mishap
- Resolution: safety analyses must include the message priority structure and determine those messages that require higher priorities to preclude transitions to hazardous modes, sub-modes, states or combinations and return the system to a safe state.

1. Not all safety-critical messages will require higher priority

SoS: Priority Structure

- Resolution continued
- Precepts
  - Not covered by current precepts
  - Loosely related to data integrity, data senescence, race conditions
  - DSP (new): Priority message processing shall ensure that the UV cannot transition to or remain in an unsafe mode, sub-mode, state or combination thereof and ensure that the system transitions to a safe mode, sub-mode, state or combination thereof in a timely manner.
  - Pass to C2 group for refinement

SoS: Race Conditions

- Issue: race conditions affect the quality and latency of data and control functions
- Rationale: race conditions can result in a number of issues including loss of situational awareness, errors in command and control, commands occurring out of sequence, etc.
- Race Conditions may lead to any of the TLMs

SoS: Race Condition

- Resolution: See data latency/ senescence, Priority structure issues

SoS: Error in UV selection/ data transfer

- Issue: Operator must be fully aware of UV situation and context (including environment) when assuming control of UV
- Rationale: selection and/ or transfer of control of incorrect UV may result in hazardous conditions
  - e.g., Selection of incorrect UGV results in vehicle running over friendly troops
- Resolution: Referred to situational awareness and C2 working groups

SoS: Control security

- Issue: Loss of control of UV due to hostile intervention
- Rationale: See data security
- Referred to C2 Working Group

SoS: Control transfer

- See control transfer

SoS: IFF/ Friendly fire mitigation

- Referred to C2 working group